The Claims

1-28. (Canceled).

29. (Original) A system comprising:

a control module to obtain an access control entry corresponding to a file to be accessed by the system, wherein the access control entry includes a symmetric key encrypted with a public key of a public/private key pair;

a key cache to maintain a plurality of mappings each of which maps an access control entry to a symmetric key;

a comparator, communicatively coupled to the control module, to check whether one of the plurality of mappings corresponds to the received access control entry; and

a cryptographic engine, communicatively coupled to the control module, to:

use, if one of the plurality of mappings corresponds to the received access control entry, the symmetric key to which the received access control entry maps to decrypt the file, and

use, if one of the plurality of mappings does not correspond to the received access control entry, the private key of the public/private key pair to decrypt the symmetric key, and then use the decrypted symmetric key to decrypt the file.

30. (Original) A system as recited in claim 29, wherein the system is a computing device in a serverless distributed file system.

31. (Original) A system as recited in claim 29, wherein the system is a computing device in a centralized distributed file system.

32. (Original) A system as recited in claim 29, wherein the control module is further to:

receive an access control list including a plurality of access control entries;

select one of the plurality of access control entries that corresponds to a user of the system; and

use, as the access control entry, the selected one of the plurality of access control entries.

33. (Original) A system as recited in claim 29, wherein the control module is further to create, if one of the plurality of mappings does not correspond to the received access control entry, a new mapping in the key cache that maps the access control entry to the symmetric key.

34. (Original) A system as recited in claim 29, wherein:

the cryptographic engine is further to encrypt, using the private key, another file including the key cache; and

the control module is further to store the encrypted file.

35. (Original) A system as recited in claim 29, wherein:

the cryptographic engine is further to encrypt, using another symmetric key, another file including the key cache, and to encrypt, using the private key, the other symmetric key; and

the control module is further to generate a new access control entry corresponding to the other file, and to store both the encrypted other symmetric key and an identifier of a user corresponding to the key cache in the new access control entry.

36. (Original) A system as recited in claim 29, wherein the control module is further to:

obtain a key cache in encrypted form from a remote storage device;

decrypt the key cache using the private key; and

use, as the key cache, the decrypted key cache.

37-44. (Canceled).